http://www.citer.wvu.edu/members/publications/files/15-SSchuckers-Elsevior02.pdf (Dec. 20, 2002) (and references cited therein), each incorporated by reference herein.

FIG. 3 is a flow chart describing an exemplary implementation of a watermark encoding process 300 in accordance with the present invention. The watermark encoding process 300 can be performed by the watermark encoding processor 120 of FIG. 1 to insert a watermark into content data 110. As shown in FIG. 3, the watermark encoding process 300 is initiated during step 310 when a user requests to obtain a copy of the content 110. Biometric and system information are obtained from the user during step 320. The obtained biometric watermark may include, for example, a finger print, speech pattern, iris pattern, or facial image. The biometric and system information are embedded in the content during step 330 using known watermarking techniques, such as those described in International Patent No. WO 08/091375, entitled "Watermarking." Generally, the biometric image can be treated like any image, such as a corporate logo, for which well known techniques exist for embedding image-based watermarks in content. As previously indicated, multiple instances of the biometric can optionally be taken and embedded into the content.

FIG. 4 is a flow chart describing an exemplary implementation of a watermark detection process 400 in accordance with the present invention. The watermark detection process 400 can be performed by the watermark detector 210 of FIG. 2. As shown in FIG. 4, the watermark detection process 400 is initiated during step 410 when a user attempts to access content protected by a biometric watermark in accordance with the present invention. A test is performed during step 420 to determine if the content has previously been authorized on the current system, using, for example, the system parameters that were embedded into the biometric watermark. If it is determined during step 420 that the content has previously been authorized on the current system, then the user is allowed to access the content during step 430.

If, however, it is determined during step 420 that the content has not previously been authorized on the current system, then a live biometric is obtained from the user during step 440. A further test is performed during step 450 to determine if the live biometric matches the biometric that was embedded in the content as a biometric watermark. If it is determined during step 450 that the live biometric matches the

biometric that was embedded in the content as a biometric watermark, then the user is allowed to access the content during step 460. In addition, the system parameters for the new system can optionally be embedded in a new biometric watermark in the content. If, however, it is determined during step 330 that the live biometric does not match the biometric that was embedded in the content as a biometric watermark, then the user is not allowed to access the content and program control terminates during step 470.

It is to be understood that the embodiments and variations shown and described herein are merely illustrative of the principles of this invention and that various modifications may be implemented by those skilled in the art without departing from the scope and spirit of the invention.